Method and Apparatus for Modular Multiplication

ABSTRACT

In a method for modular multiplication of a multiplicand by a multiplier using a modulus, l multiplication shift values are initially determined by means of a multiplication-lookahead method while taking into account l blocks of consecutive digits of the multiplier. Subsequently, l reduction shift values are determined by means of a reduction-lookahead method for the l blocks of digits of the multiplier. The l multiplication shift values and the l reduction shift values are applied to an intermediate result from a previous iteration step, to the modulus or to a value derived from the modulus, and to the multiplicand, so as to obtain the 2l+1 operands. By means of a multi-operands adder, the 2l+1 operands are combined to obtain an updated intermediate result for an iteration step following the previous iteration step, the iteration being continued for such time until all digits of the multiplier have been processed. Depending on the number of operands, the number of cycles to be calculated is reduced, so that faster calculation of the modular multiplication is possible at the expense of higher hardware expenditure.